OneCommand® Manager Application for Solaris Release Notes

Version: 10.4.255.16

System: Solaris 10, 11, 12 (64-bit, x86, and SPARC)

Date: March 2015

Purpose and Contact Information

These release notes describe the new features, resolved issues, known issues, and technical tips associated with this OneCommand™ Manager application version for the Emulex® drivers for Solaris.

For the latest product documentation, go to www.Emulex.com. If you have questions or require additional information, contact an authorized Emulex technical support representative at tech.support@emulex.com, 800-854-7112 (US/Canada toll free), +1 714-885-3402 (US/International), or +44 1189-772929 (Europe, Middle East, and Africa).

New Features

1. **Supports OCe14000-series 10GBASE-T adapters**
2. **Dropped support for OCe10100-series adapters**

Resolved Issues

1. **Enabling or disabling boot on LPe16000-series adapters no longer displays an error message.**
2. **For the LPe16000-series adapters, if an external loopback plug is connected to the system, the D_Port test runs correctly.**
3. **The OneCommand Manager CLI GetQoSInfo command no longer shows incorrect units.**
4. **For OCe14000-series adapters with an OCe11102 TCP offload, Mutual CHAP credentials are no longer inverted in the OneCommand Manager application.**
5. **For PFC (priority-based flow control), active priority information is now correct.**
6. **The *OneCommand Manager CLI User Manual* no longer incorrectly states that the DMA loopback test is supported on the LPe16202 adapters.**

Known Issues

1. **Known Issues related to updating firmware.**

   a) The 10.4 firmware versions include new features that require new flash regions to support them. Firmware versions earlier than 10.0.803.37 did not have the ability to configure the flash regions to support these new features.

   If you are updating from a firmware version earlier than 10.0.803.37, use one of these methods to update the 10.4 firmware:

   - Use the ISO flash tool.
   - Use the released 10.4 version of the OneCommand Manager application GUI or OneCommand Manager CLI application. You must perform the firmware update procedure twice to ensure that the flash regions are properly configured, and you must reboot the system after each firmware update.

   Note: After you have updated the firmware, you must not downgrade the firmware to a version earlier than 10.0.803.37.

2. **For the LPe16000-series adapters, if a diagnostic test (OneCommand Manager application or OneCommand Manager CLI) determines that the switch does not support D_Port, the port remains in D_Port mode.**

   Workaround

   Manually reset the port.

3. **For OCe14000-series adapters, on the Physical Port Info tab, the Set Speed button may be inactive.**

   Workaround

   None.

4. **The OneCommand Manager CLI PortAttributes command reports the wrong VEPA state on SPARC clients.**

   Workaround

   Use the OneCommand Manager application GUI.

5. **For OCe14000-series adapters, the OneCommand Manager CLI SetAdapterPortConfig command fails on SPARC clients.**

   The SetAdapterPortConfig command fails and shows "ERROR: the NIC protocol is not supported on the specified function."

   Workaround

   None.

6. **For OCe14000-series adapters, the OneCommand Manager GUI on SPARC clients shows incomplete Adapter Configuration tab information if the adapter configuration is changed.**

   The Adapter Configuration tab does not show minimum and maximum bandwidth information.

   Workaround

   None.

7. **On the Channel Management tab, the OneCommand Manager application always shows the permanent MAC address for each channel.**

   Workaround

   To correlate the permanent MAC address with the current MAC address, view the Port Information tab. The Port Information tab always shows the current (user-settable) MAC address and the permanent MAC address.

8. **The NIC driver must be installed and enabled to run the OneCommand Manager application on an FCoE OneConnect® adapter.**

   If the OneConnect FCoE adapter is run without the NIC driver installed and enabled, many of the management functions are unavailable and erroneous/corrupted information is displayed by the OneCommand Manager application.

   Unavailable management functions include:

   - Downloading
   - All diagnostics, including beaconing and diagnostic dumps
   - Core Dump
   - Disabling or enabling a port

   Erroneous or corrupt display information includes:

   - FCoE storage ports are incorrectly grouped under the physical port
   - NIC, FCoE, and iSCSI ports do not appear under the correct adapter
   - Active and flash firmware versions
   - Firmware status
   - BIOS version
   - Boot code version
   - Transceiver data display
   - Physical port link status
   - All DCB settings
   - Event log display (OneCommand Manager CLI only)

   Workaround

   Install and enable the NIC driver before running the OneCommand Manager application GUI or OneCommand Manager CLI.

9. **Changing the channel management mode may disrupt network traffic.**

   When the channel management mode of the OneConnect CNA is changed from SIMode to vNIC1 mode, the existing SIMode LPVID settings carry over to the vNIC1 LPVID settings (also called Inner VLAN ID settings). This carry over may disrupt network traffic. The OneCommand Manager application GUI and OneCommand Manager CLI do not allow you to change the vNIC1 LPVIDs.

   Workaround

   Use the Emulex PXESelect Utility to set the vNIC1 LPVID value:

   a) Start or reboot the system. When prompted, hold down **<Ctrl>** and press **<P>** to enter the Emulex PXESelect Utility.

b) In the Controller Configuration menu, press **<Tab>** until **Continue** is highlighted. Press **<Enter>**.

c) Select the adapter and port number to be configured and press **<Enter>**.

d) Under the MultiChannel Configuration menu, set the LPVID for each NIC channel to either 0 (default) or the desired value. Press **<Tab>** until **Save** is highlighted and press **<Enter>**.

e) Continue to press **<Esc >** until prompted with the message: "Do you want to exit from the utility?"

f) Press **<Y>** to exit.

10. A reboot is required if you change the volatile WWN on an LPe16000-series adapter.

Workaround

None.

11. Rebooting the system after a firmware update does not activate the new firmware.

Workaround

- Perform a standard reboot using one of the following methods:
  - Issue the reboot –p command.
  - Configure the boot-config service to issue the standard reboot by default.
  - On x86 platforms running Solaris 11, disable Fast Reboot.

  Note: See the Solaris documentation for more details on Fast Reboot.

- If a standard reboot does not resolve the issue, power cycle the system.

12. While running the OneCommand Manager application and during high converged I/O traffic, a panic can occur when enabling or disabling Ethernet switch ports.

Workaround

Stop the OneCommand Manager application daemons before enabling or disabling Ethernet ports.

13. The OneCommand Manager application GUI and the OneCommand Manager CLI may fail to run and return an error.

The OneCommand Manager application and OneCommand Manager CLI may fail to run and return the following error:

```
ld.so.1: hbacmd: fatal: libgcc_s.so.1: open failed: No such file or
directory
```

This error is caused by an unsatisfied dependency on the GCC Runtime library.

Workaround

Install the SUNWgccruntime package.

14. When you install the OneCommand Manager application on a guest operating system, the installer prompts you for a management mode.

When installing the OneCommand Manager application on a guest operating system running on a virtual machine, the installer prompts you for a management mode (e.g. local-only, full-remote, etc.) and read-only mode. However, when the OneCommand

Manager application runs on a guest operating system it runs in local-only and read-only modes, so it does not matter how these modes are specified during installation.

Workaround

None.

15. **OneCommand Manager Secure Management mode on Solaris systems require PAM authentication configuration on the host machine.**

    In Secure Management mode, a user is authenticated on the machine at OneCommand Manager application GUI startup. This is handled via the PAM interface.

    Workaround

    Place the correct setting in the "auth" section of /etc/pam.d/other file or its earlier equivalent, /etc/pam.conf. Refer to the *OneCommand Manager Application User Manual* for more information about Secure Management mode.

16. **The OCe11101-E CNA cannot run loopback diagnostic tests (PHY, MAC, External). Any attempt to run a loopback test on the OCe11101-E CNA results in failure.**

    Workaround

    None.

17. **OneCommand Manager Secure Management Group Assignment/Configuration on Solaris using the useradd command requires a -G option.**

    If you assign users to one of the four OneCommand Manager application groups using the useradd command, using the -g option instead of the -G option results in the user membership data not being returned in the getent group command and associated OneCommand Manager Secure Management code failure to retrieve OneCommand Manager application user group membership data (and thus provide privileges to user).

    Workaround

    Use the -G option instead.

18. **On OCe11100-series adapters, if the Mode is set to Force and the Speed is set to 1 Gb per second (Gbps), do not perform a MAC loopback test using the OneCommand Manager application.**

    The Mode and Speed can be set from the Physical Port info tab in the OneCommand Manager application or with the SetPhyPortSpeed OneCommand CLI command. If you perform a MAC loopback test, the link does not come back up after the test is performed.

    Workaround

    None.

19. **On Solaris 10 systems, the OneCommand Manager application, OneCommand Manager CLI, and all OneCommand Manager services may not run. The following error message appears:**

    ```
    "HBA_LoadLibrary: previously unfreed libraries exist, call
    HBA_FreeLibrary()"
    ```

    The problem may be caused by devices on the SAN behaving incorrectly. This has been seen only on Solaris 10 x86 and SPARC platforms, beginning with update 6.

Workaround

Any one of the following solutions may correct this problem.

- Reboot the system.
- Check for any malfunctioning adapters.
- Check SAN infrastructure for connections or elements that may create excessive network latency. Make adjustments and reduce complexity where possible.
- Remove unneeded virtual ports.

20. The OneCommand Manager application, OneCommand Manager CLI, and all OneCommand Manager services are unable to run. The following error message repeatedly prints to the syslog and/or console:

```
"ElxInitBrdMap: HBAAPI initialization attempt failed"
```

This known issue occurs when the HBAAPI fails to report all adapters in the system.

Workaround

This known issue often resolves itself after several minutes. If the problem does not resolve itself, the following actions may resolve the problem:

- Reboot the system.
- Check for any malfunctioning adapters.
- Check SAN infrastructure for connections or elements that may create excessive network latency. Make adjustments and reduce complexity where possible.
- Remove unneeded virtual ports.

21. If a system contains several HBAs or CNAs and is experiencing slow performance, the elxhbamgrd service may fall into a "maintenance" state during boot. This would prevent the system from being managed by a remote OneCommand Manager application client.

Workaround

Any one of the following solutions may correct this problem.

- Remove any unused HBAs or CNAs.
- After each reboot, restart the OCM services using the commands:

  ```
  /opt/ELXocm/stop_ocmanager
  ```

  ```
  /opt/ELXocm/start_ocmanager
  ```

- After each reboot, restart the elxhbamgrd service using the commands:

  ```
  svcadm disable elxhbamgrd
  ```

  ```
  svcadm enable elxhbamgrd
  ```

22. The Web Launch browser client must be run with administrator/root privileges.

When running the OneCommand Manager Web Launch GUI, you must have administrator privileges when logged into the Web Launch client. On Solaris browser clients, you must be logged in as the 'root' user. Unusual behavior may occur if this requirement is not met.

Workaround

None.

23. Set Link Speed Issue after SFP Hot Swap

LPe16000-series adapters do not support SFP hot swap if the replacement SFP is not the same model as the original SFP. There are two ramifications in the OneCommand Manager application:

1. The Port Attributes tab in the OneCommand Manager application GUI or the OneCommand Manager CLI PortAttributes command may display incorrect data for the Supported Link Speeds attribute. This issue is cosmetic.
2. Boot From SAN management may be unable to set the Boot Code Link Speed parameter to 16 Gbps.

Workaround

After changing the SFP, reset the LPe16000-series adapter port or reboot the server.

24. The discovery refresh interval that can be set in the OneCommand Manger's Discovery Settings dialog does not change the discovery interval for the adapters on the local system. The refresh interval for local devices is 45 seconds.

Workaround

None.

25. When using FC adapters with the OneCommand Manager, the SLI-1 is always unavailable.

Workaround

None.

26. When performing a PHY loopback test in the OneCommand Manager application on an Emulex OCe14102-NT or OCe14102-UT adapter, the test may fail after a random period of time.

Workaround:

None.

27. When using OCe14000-series adapters, the Apply button may disabled in the Adapter Configuration tab when changing from a custom concurrent storage configuration to a single storage personality.

Workaround

Use the Custom view rather than the Single Personality view to change the next boot configuration.

28. When a host is added on the remote system for Solaris 11.2, the remote OneCommand Manager application GUI does not discover the added host.

Workaround

None.

29. Core dump is not supported on the FC/FCoE driver for Solaris SPARC. (BZ 174474)

Workaround

None.

Technical Tips

1. **The OneCommand Manager CLI UmcEnableChanLink command has been removed.**

   To enable the logical link status of a channel, use the CMSetBW command to set the minimum bandwidth to a value greater than 0. To disable the logical link status, set the minimum bandwidth to 0.

2. **Roles based Secure Management mode is available.**

   Secure Management mode is a management mode available with this release. It is a roles based security implementation. During the OneCommand Manager application installation, a user is prompted as to whether or not to run in Secure Management mode. When the OneCommand Manager application is installed in this mode, the following operational changes occur:

   - A non-root or non-administrator user can run the OneCommand Manager application.
   - The OneCommand Manager application host uses a user's credentials for authentication.
   - A user has OneCommand Manager application configuration privileges according to the OneCommand Manager application group to which the user is assigned.
   - In Secure Management mode, a root or administrator user is provided full privileges on the local machine (OneCommand CLI does not require credentials) but no remote privileges.

   Note: Refer to the *OneCommand Manager Application User Manual* for more information on Secure Management mode.

3. **OneCommand Manager Secure Management mode requires OneCommand Manager user groups to be configured on the domain or if the host is not running in a domain, the host machine.**

   OneCommand Manager Secure Management must be able to get the OneCommand Manager application group to which the user belongs from the host's domain (Active Directory or Lightweight Directory Access Protocol [LDAP]) or if the host is not part of a domain, the host's local user accounts. This access is associated with the user groups, not with specific users. An administrator needs to create these user groups and then set up user accounts such that a user belongs to one of these four OneCommand Manager application user groups:

   Table 1 Secure Management User Privileges

User Group	OneCommand Manager Capability
ocmadmin	Allows full active management of local and remote adapters.
ocmlocaladmin	Permits full active management of local adapters only.
ocmuser	Permits read-only access of local and remote adapters.
ocmlocaluser	Permits read-only access of local adapters.

   These four OneCommand Manager application groups must be created and configured on the host machine or network domain. OneCommand Manager Secure Management uses the C-library API calls getgrnam and getgrid to retrieve the OneCommand Manager Secure Management group information. The equivalent to these can be obtained on the shell command line by typing getent group command. If the four OneCommand Manager

application groups are listed, along with their member users, this is an indication that the host machine is sufficiently configured to work with OneCommand Manager Secure Management.

4. **FC in-band management is no longer supported.**
5. **The OneCommand Manager application no longer installs OneCommand Vision components.**
6. **On OneConnect adapters, if you change the port speed via the Change Port Speed dialog box, and the selected speed is supported by the adapter's port but is not supported by the connected hardware, the link does not come up.**
7. **Requirement if DCB settings are connected to a non-data center bridging exchange (DCBX) switch.**

   If DCB settings are required when connected to a non-DCBX switch (or switch with DCBX disabled), DCBX must be disabled on the OneConnect adapter to use the adapter's configured parameters. If DCBX is enabled, the DCB PFC and Priority Groups are ignored (the adapter assumes that the switch does not support these parameters) and for FCoE adapters, the FCoE priority (COS) is 3.
8. **The OneCommand Manager application Firmware tab is in a different location for 8 Gb and lower Fibre Channel adapters than it is for 16 GFC adapters and OneConnect CNAs.**

   Because the 16 GFC adapters and OneConnect CNAs share a single firmware image for all ports on the adapter, the Firmware tab for them is at the adapter level. Because 8 GFC and lower adapters have a separate firmware images for each individual port, the Firmware tab for them is at the port level.
9. **DH-CHAP authentication is no longer supported.**
10. **To view online help using the Google Chrome browser, you must disable Chrome's security check using the "--allow-file-access-from-files" option.**
    a) Create a copy of the Chrome shortcut on the desktop and rename it to RH Chrome L
    b) Right-click on the new Chrome icon and choose **Properties**.
    c) Add the "--allow-file-access-from-files" text to the end of the path appearing in Target. You must leave a space between the original string and the tag you are adding to the end of it.
    d) Click **OK** to save your settings.
    e) Close any open instances of Chrome.
    f) To open a local copy of the online help, use the new shortcut to open Chrome, then hold down **<Ctrl>** and press **Open** and browse to the start page; or open Chrome with the new shortcut, then right-click the start page and click **Open With > Google Chrome**.
11. **The OneCommand Manager application supports a maximum of 16 ASICs for OneConnect adapters. Most OneConnect adapters have a single ASIC, so a maximum of 16 adapters can be seen and managed by the OneCommand Manager application. There are some OneConnect adapter models that have two ASICs. When all the adapters have two ASICS, a maximum of eight adapters can be seen and managed by the OneCommand Manager application.**

12. SR-IOV is not supported by the OneCommand Manager application. SR-IOV management is provided through the Solaris operating system.

Note: References to OCe11100-series products also apply to OCe11100R series products.